

# WSA2 - HTTP

## 1

```
✓ Hypertext Transfer Protocol
  ✓ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr,en;q=0.9,en-gb;q=0.8,en-us;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

Version: 1.1

Languages: tr, en, en-gb, en-us

No.	Time	Source	Destination	Protocol	Length	Info
97	2.911746	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
126	3.062169	128.119.245.12	192.168.1.25	HTTP	540	HTTP/1.1 200 OK (text/html)

Ip address of my computer: 192.168.1.25

Ip address of http server: 128.119.245.12

```
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    ✓ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

Status code: 200

Status phrase: OK

```
✓ Hypertext Transfer Protocol
  ✓ HTTP/1.1 200 OK\r\n
    ✓ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Sat, 21 Oct 2023 17:28:51 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Pe
      Last-Modified: Sat, 21 Oct 2023 05:59:01 GMT\r\n
      ETag: "80-60833af8df455"\r\n
```

Date: 10/21/2023

Time: 05:59:01

```
      ETag: "80-60833af8df455"\r\n
      Accept-Ranges: bytes\r\n
    > Content-Length: 128\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
```

128 bytes of content are being returned to my browser.

2

http						
No.	Time	Source	Destination	Protocol	Length	Info
60	2.161235	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
90	2.312486	128.119.245.12	192.168.1.25	HTTP	784	HTTP/1.1 200 OK (text/html)
108	2.393353	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
110	2.563476	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)
147	12.861716	192.168.1.25	128.119.245.12	HTTP	666	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
152	13.012293	128.119.245.12	192.168.1.25	HTTP	294	HTTP/1.1 304 Not Modified

  

```
\r\n
[HTTP response 1/2]
[Time since request: 0.151251000 seconds]
[Request in frame: 60]
[Next request in frame: 108]
[Next response in frame: 110]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server \n
```

The first HTTP GET request does not contain “if-modified-since” line.

The server returned full contents of file in 200 OK reply message.

http						
No.	Time	Source	Destination	Protocol	Length	Info
49	2.147920	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
67	2.299567	128.119.245.12	192.168.1.25	HTTP	784	HTTP/1.1 200 OK (text/html)
84	2.377227	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
106	2.528281	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)
170	12.426354	192.168.1.25	128.119.245.12	HTTP	666	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
189	12.583156	128.119.245.12	192.168.1.25	HTTP	294	HTTP/1.1 304 Not Modified

  

```
> Internet Protocol Version 4, Src: 192.168.1.25, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50988, Dst Port: 80, Seq: 1, Ack: 1, Len: 612
  Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: tr,en;q=0.9,en-G8;q=0.8,en-US;q=0.7\r\n
      If-None-Match: "173-60833af8dec85"\r\n
      If-Modified-Since: Sat, 21 Oct 2023 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 189]
```

The second HTTP GET request contains “If-Modified-Since” line.

```
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
If-None-Match: "173-60833af8dec85"\r\n
If-Modified-Since: Sat, 21 Oct 2023 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 152]
```

A date and time stamp.

No.	Time	Source	Destination	Protocol	Length	Info
60	2.161235	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
90	2.312486	128.119.245.12	192.168.1.25	HTTP	784	HTTP/1.1 200 OK (text/html)
108	2.393353	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
110	2.563476	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)
147	12.861716	192.168.1.25	128.119.245.12	HTTP	666	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
152	13.012293	128.119.245.12	192.168.1.25	HTTP	294	HTTP/1.1 304 Not Modified

  

▼ HTTP/1.1 304 Not Modified\r\n	0000 e4 a
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]	0010 01 1
[HTTP/1.1 304 Not Modified\r\n]	0020 01 1
[Severity level: Chat]	0030 00 e
[Group: Sequence]	0040 30 3
Response Version: HTTP/1.1	0050 0a 4
Status Code: 304	0060 63 7
[Status Code Description: Not Modified]	0070 20 4
Response Phrase: Not Modified	0080 61 6
Date: Sat, 21 Oct 2023 18:53:08 GMT\r\n	0090 4f 5
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n	00a0 32 6l
Connection: Keep-Alive\r\n	00b0 33 3
Keep-Alive: timeout=5, max=100\r\n	00c0 31 3
ETag: "173-60833af8dec85"\r\n	00d0 0a 4
\r\n	00e0 70 2
[HTTP response 1/1]	00f0 69 7l
[Time since request: 0.150577000 seconds]	0100 6d 6
[Request in frame: 147]	0110 31 3
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]	0120 35 2

The server did not return the full contents of file with “304 Not Modified” reply message.

3

No.	Time	Source	Destination	Protocol	Length	Info
391	4.477414	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
456	4.628457	128.119.245.12	192.168.1.25	HTTP	679	HTTP/1.1 200 OK (text/html)
465	4.720409	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
477	4.871082	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

My browser sent 1 request message in order to download the lengthy US Bill of Rights and its packet number is 391. The server replied it with status code 200 and status phase OK on packet number 456.

```

> Frame 456: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface \Device\NPF_{DC50A74E-...}
> Ethernet II, Src: HuaweiTe_53:78:6a (94:25:33:53:78:6a), Dst: LiteonTe_e0:ed:b3 (e4:aa:ea:e0:ed:b3)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.25
> Transmission Control Protocol, Src Port: 80, Dst Port: 51477, Seq: 4237, Ack: 501, Len: 625
> [4 Reassembled TCP Segments (4861 bytes): #453(1412), #454(1412), #455(1412), #456(625)]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sat, 21 Oct 2023 20:25:23 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

```

4 TCP segments.

4

No.	Time	Source	Destination	Protocol	Length	Info
556	3.423883	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
598	3.574333	128.119.245.12	192.168.1.25	HTTP	1355	HTTP/1.1 200 OK (text/html)
612	3.593310	192.168.1.25	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
648	3.737238	192.168.1.25	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
651	3.744967	128.119.245.12	192.168.1.25	HTTP	841	HTTP/1.1 200 OK (PNG)
663	3.802455	178.79.137.164	192.168.1.25	HTTP	225	HTTP/1.1 301 Moved Permanently
722	4.103381	192.168.1.25	212.252.126.88	HTTP	372	GET /roots/dstrootcax3.p7c HTTP/1.1
728	4.114545	212.252.126.88	192.168.1.25	HTTP	1460	HTTP/1.1 200 OK
1267	4.591470	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
1290	4.742416	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

4 HTTP GET request messages.

No.	Time	Source	Destination	Protocol	Length	Info
556	3.423883	192.168.1.25	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
598	3.574333	128.119.245.12	192.168.1.25	HTTP	1355	HTTP/1.1 200 OK (text/html)
612	3.593310	192.168.1.25	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
648	3.737238	192.168.1.25	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
651	3.744967	128.119.245.12	192.168.1.25	HTTP	841	HTTP/1.1 200 OK (PNG)
663	3.802455	178.79.137.164	192.168.1.25	HTTP	225	HTTP/1.1 301 Moved Permanently
722	4.103381	192.168.1.25	212.252.126.88	HTTP	372	GET /roots/dstrootcax3.p7c HTTP/1.1
728	4.114545	212.252.126.88	192.168.1.25	HTTP	1460	HTTP/1.1 200 OK
1267	4.591470	192.168.1.25	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
1290	4.742416	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Exactly two different HTTP GET request went to 128.119.245.12 on 556 and 612. One additional http GET request went to 178.79.137.164 and it returns 301 Object moved code. So, fourth one went to 212.252.126.88.

5

No.	Time	Source	Destination	Protocol	Length	Info
543	3.090732	192.168.1.25	128.119.245.12	HTTP	570	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
589	3.246340	128.119.245.12	192.168.1.25	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2258	14.344468	192.168.1.25	128.119.245.12	HTTP	655	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
2291	14.495504	128.119.245.12	192.168.1.25	HTTP	544	HTTP/1.1 200 OK (text/html)
2300	14.582471	192.168.1.25	128.119.245.12	HTTP	516	GET /favicon.ico HTTP/1.1
2320	14.739260	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet number of the first HTTP GET request is 543. The server's response is 401 Unauthorized.

http						
o.	Time	Source	Destination	Protocol	Length	Info
543	3.090732	192.168.1.25	128.119.245.12	HTTP	570	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm
589	3.246340	128.119.245.12	192.168.1.25	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
2258	14.344468	192.168.1.25	128.119.245.12	HTTP	655	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.htm
2291	14.495504	128.119.245.12	192.168.1.25	HTTP	544	HTTP/1.1 200 OK (text/html)
2300	14.582471	192.168.1.25	128.119.245.12	HTTP	516	GET /favicon.ico HTTP/1.1
2320	14.739260	128.119.245.12	192.168.1.25	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (601 bytes)
· Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 Edg/118.0.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
    \r\n

```

Authorization field is included in the second HTTP GET message.